PTO/SB/08A (07-06)
Approved for use through 09/30/2006. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE

Substitute for form 1449A/PTO

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Use as many sheets as necessary)

Sheet	1	of	2

Complete if Known	
Application No/Application No	09/844,447/7,089,428
Filing Date	April 27, 2001
First Named Inventor	Timothy P. Farley
Art Unit	2132
Examiner Name	Zand, Kambiz
Attorney Docket Number	05456.105006

FOREIGN PATENT DOCUMENTS

Examiner Initials*	Cite No.[1]	Foreign Patent Document Country Code[3] - Number[4] - Kind Code[5] (*if known*)	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear	T[6]
	1.	WO 99/13427	03-18-1999	MCI WORLD-COM, INC.	Page No. 60-69, Claims 12, 32, 33, and 36	
	2.	WO 01/84285	08-11-2001	Internet Security Systems, Inc.	Page No. 59-63, Claims 7, 8, 14, and 22	

NON PATENT LITERATURE DOCUMENTS

Examiner Initials *	Cite No.[1]	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published.	T [2]
	3.	CROSBIE, MARK et al., Active Defense of a Computer System Using Autonomous Agents, COAST Group Dept. of Computer Sciences Purdue, 1995, No. 95-008, “citeseer.ist.psu.edu/138521.html” [Pertinent: Pg. 10, paragraph 7]	
	4.	DENNING, D.E., An Intrusion-Detection Model, Software Engineering, IEEE Transactions on: Vol. SE-13, Issue 2, Feb. 1987 Pgs. 222-232. [Pertinent: Pgs. 5-14, paragraph V]	
	5.	PORRAS, P.A. et al, Penetration State Transition Analysis: A Rule-Based Intrusion Detection Approach, Computer Security Applications Conference, 1992, Proceedings, Eighth Annual Nov. 30 -Dec. 4, 1992, pgs. 220-229. [Pertinent: Pgs. 222-226 and paragraph 3]	
	6.	LINDQVIST, U. et al., eXpert-BSM: a host-based intrusion detection solution for Sun Solaris, Computer Security Applications Conference, 2001. ASCAC 2001, Proceedings 17th Annual, Dec. 10-14, 2001, Pgs. 240-251. [Pertinent: Pgs. 3-6, paragraph 3]	
	7.	ICE Cap Administrator's Guide Version 1.0 BETA, NETWORK ICE, 1999, Network Ice Corporation. [Pertinent pages 27-33, paragraph 4]	
	8.	DENNING, P. NEUMANN, Requirements and Model for IDES Real Time Intrusion Detection Expert System, SRI Project 6169, Final Report, August 1985. [Pertinent pages 11-12, paragraphs 3.3-3.3.1]	
	9.	TENG, H.S., et al., Adaptive Real-Time Anomaly Detection Using Inductively Generated Sequential Patterns, Research in Security and Privacy, 1990., Proceedings., 1990 IEEE Computer Society Symposium on May 7-9, 1990, pages 278-284. [Pertinent: Page 279, paragraphs 2-2.1]	
	10.	MUNSON, J.C., et al., Watcher: the missing piece of the security puzzle, Computer Security Applications Conference, 2001. ACSAC 2001. Proceedings 17th Annual, Dec. 10-14, 2001, pages 230-239. [Pertinent paragraphs 5.1-5.7]	
	11.	VALDES, AL., Blue Sensors, Sensor Correlation, and Alert Fusion, Oct. 4, 2000., http://www.raid-symposium.org/raid2000/Materials/Abstracts/41/avaldes_raidB.pdf. [Pertinent: Charts 5-8]	
	12.	NetRanger User's Guide Version 2.1.1, Cisco Systems, Inc., 1998. [Pertinent: Pages 4-62 to 4-95, paragraph 4]	
	13.	PORRAS, PHILLIP, et al., Mission-Impact-Based Approach to INFOSEC Alarm Correlation, Lecture Notes in Computer Science, Proceedings Recent Advances in Intrusion Detection, October 2002, pages 95-114. [Pertinent: 2-8, paragraphs 2-2.4.1]	
	14.	BACE, REBECCA, An Introduction to Intrusion Detection & Assessment for System and Network Security Management, Infidel, Inc. for ICSA (White Paper) April 1999. [Pertinent: Pages 23-32]	
	15.	BASS, TIM, Multisensor Data Fusion for Next Generation Distributed Intrusion Detection Systems, Proceedings, 1999 IRIS National Symposium on Sensor and Data Fusion, May 1999. [Pertinent: Pages 2-6, paragraphs III-V]	
	16.	LUCKHAM, DAVID C., et al., Complex Event Processing in Distributed Systems, Stanford University Technical Report CSL-TR-98-754, March 1998, 28 pages. [Pertinent: Pages 4-8, Paragraph 2].	

Examiner Signature		Date Considered	

PTO/SB/08A (07-06)
Approved for use through 09/30/2006. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE

Substitute for form 1449A/PTO

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Use as many sheets as necessary)

Sheet 2 of 2

Complete if Known	
Application No/Application No	09/844,447/7,089,428
Filing Date	April 27, 2001
First Named Inventor	Timothy P. Farley
Art Unit	2132
Examiner Name	Zand, Kambiz
Attorney Docket Number	05456.105006

NON PATENT LITERATURE DOCUMENTS

Examiner Initials *	Cite No.[1]	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published.	T[2]
	17.	CUPPENS, FREDERIC, Cooperative Intrusion Detection, ONERA Centre de Toulouse (funded by the DGA/CASSI). [Pertinent: Pages 5-9, paragraphs 5-7]	
	18.	MUKHERJEE, B., Network Intrusion Detection, IEEE Network Magazine: May/June 1994, Volume: 8, Issue: 3, pages 26-41. [Pertinent: Page 38].	
	19.	BASS, TIM, Intrusion Detection Systems and Multisensor Data Fusion, Communications of the ACM, Volume 43, Issued 4 (April 2000), pages 99-105. [Pertinent: Pages 101-104]	
	20.	Rationalizing Security Events with Three Dimensions of Correlation, netForensics inc. 2005, Tech brief, http://www.netforensics.com/download/nF_Comprehensive_Correlation.pdf. [Pertinent: Pages Nos. 1-6]	
	21.	METCALF, THERESE R., Intrusion Detection System Requirements, MITRE PAPER. A Capabilities Description in Terms of the Network Monitoring and Assessment Module of CSAP21, September 2000. [Pertinent: Page Nos. 5-8, Paragraph 3]	
	22.	JOU, FRANK Y., et al., Architecture Design of a Scalable Intrusion Detection System for the Emerging Network Infrastructure, DARPA, Order Number: E296, April 1997, http://citeseer.ist.psu.edu/jou97architecture.html. [Pertinent: page 19, paragraphs 4.3.3.1.1]	
Examiner Signature		Date Considered	